UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/719,460	12/11/2000	Tomoyuki Asano	450101-02452	8319

20999 7590 07/14/2005

FROMMER LAWRENCE & HAUG
745 FIFTH AVENUE- 10TH FL.
NEW YORK, NY 10151

EXAMINER	
TRAN, TONGOC	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 07/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/719,460	ASANO ET AL.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-107* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-107* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on 2/28/2005. Claims 1, 28, 55 and 82 have been amended. Claims 1-107 are pending.

Response to Arguments

2. Applicant's arguments with respect to amended claims 1, 28, 55 and 82 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-107 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traw et al. (U.S. Patent No. 6,542,610) in view of Nguyen (U.S. Patent No. 5,689,566).

In respect to claim 1, Traw discloses an information processing system comprising: a first information processing apparatus comprising an interface having a first transmission mode in which a transmission band is ensured and a second transmission mode in which a transmission band is not ensured, and transmission control means for encrypting data requiring the assurance of the transmission band by a first encryption key and then transmitting the data in the first transmission mode via the interface and for encrypting related data relating to the data by a second encryption key

and then transmitting the related data in the second transmission mode via the interface (e.g. Abstract and col. 10, lines 28-34) ; and a second information processing apparatus comprising an interface having a first transmission mode in which a transmission band is ensured and a second transmission mode in which a transmission band is not ensured, and receiving control means for decoding, by the first encryption key, the data requiring the assurance of the transmission band which is received in the first transmission mode via the interface and for decoding, by the second encryption key, the related data received in the second transmission mode via the interface (e.g. col. Col. 4, lines 34-58 and col. 10, lines 28-34).

Straw does not disclose but Nguyen the separating means for allowing said first information processing apparatus to separate the encrypted data for transmission in either the first transmission mode or the second transmission mode; and determining means for allowing said second information processing apparatus to determine whether the received encrypted data belongs to the first transmission mode or the second transmission mode in order to perform decoding with either the first encryption key or the second encryption key (Nguyen, e.g. col. 9, line 16-col. 10, line 10). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching protecting digital content between one or more computationally constrained devices over insecure links taught by Straw with the teaching of Nguyen for providing separate means and determining means to allow data to be encrypted with different keys depending on security level of the networks for the benefit of providing

different security need according to the nature of the communication links (Nguyen, col. 1, line 58-col. 2, line 5).

In respect to claim 2, Traw and Nguyen disclose an information processing system as claimed in claim 1, wherein prior to data transmission, a protocol for performing mutual authentication and sharing a plurality of encryption keys between the first information processing apparatus and the second information processing apparatus is executed (e.g. col. 3, lines 20-30 and col. 4, lines 39-58).

In respect to claim 3, Traw and Nguyen disclose the information processing system as claimed in claim 1, wherein music data is transmitted in the first transmission mode and related data relating to the music data is transmitted in the second transmission mode (e.g. .10, lines 27-34).

In respect to claim 4, Traw and Nguyen disclose the information processing system as claimed in claim 1, wherein the first information processing apparatus and the second information processing apparatus are connected with each other via an interface conforming to the IEEE (the Institute of Electrical and Electronics Engineers) 1394 standard, for transmitting data requiring the assurance of a transmission band in an isochronous transmission mode and for transmitting related data relating to the data in an asynchronous transmission mode (e.g. col. 10, lines 27-34).

In respect to claim 5, Traw and Nguyen disclose the information processing system as claimed in claim 4, wherein prior to data transmission, a protocol for performing mutual authentication and sharing a plurality of encryption keys between the first information processing apparatus and the second information processing apparatus

is executed in an asynchronous transmission mode (e.g. col. 4, lines 39-58 and col. 6, lines 34-40).

In respect to claim 6, Traw and Nguyen disclose the information processing system as claimed in claim 1; wherein the second information processing apparatus generates two random numbers and transmits them to the first information processing apparatus, the first information processing apparatus generates two random numbers and transmits them to the second information processing apparatus, the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the first transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number, and the second information processing apparatus generates an encryption key used for decoding the data transmitted in the first transmission mode and an encryption key used for decoding the data transmitted in the second transmission mode on the basis of information indicating the validity of the apparatus itself, the generated random number and the received random number (e.g. col. 6, lines 1-66).

In respect to claim 7, Traw and Nguyen disclose the information processing system as claimed in claim 6, wherein the first information processing apparatus transmits data P generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, to the second information processing apparatus, the second information processing apparatus

transmits data Q generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, to the first information processing apparatus, the first information processing apparatus generates an encryption key used for encrypting the data to be transmitted in the first transmission mode and an encryption key used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data Q, and the second information processing apparatus generates an encryption key used for decoding the data transmitted in the first transmission mode and an encryption key used for decoding the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number is coincident with the received data P (e.g. col. 6, lines 1-67).

In respect to claim 8, Traw and Nguyen disclose the information processing system as claimed in claim 7, wherein the second information processing apparatus generates two random numbers R1 and R2 and transmits them to the first information processing apparatus, the first information processing apparatus generates two random numbers S1 and S2 and transmits them to the second information processing apparatus, the first information processing apparatus transmits data P generated on the basis of information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing

apparatus, the second information processing apparatus transmits data Q generated on the basis of information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the first information processing apparatus, the first information processing apparatus generates an encryption key K1 used for encrypting the data to be transmitted in the first transmission mode and an encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and the second information processing apparatus generates an encryption key K' I used for decoding the data transmitted in the first transmission mode and an encryption key K'2 used for decoding the data transmitted in the second transmission mode in the case where data P' generated on the basis of the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P (e.g. col. 6, lines 1-67).

In respect to claim 9, Traw and Nguyen disclose the information processing system as claimed in claim 8, wherein the first information processing apparatus generates the encryption key KI used for encrypting the data to be transmitted in the first transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number RI, and generates the encryption key KZ used for encrypting the data to be transmitted in the Second

transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, and the second information processing apparatus generates the encryption key K'1 used for decoding the data transmitted in the first transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, and generates the encryption key K'2 used for decoding the data transmitted in the second transmission mode, on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S2 and the generated random number R2 (e.g. col. 6, lines 1-67 and col. 7, lines 5-55).

In respect to claim 10, Traw and Nguyen disclose the information processing system as claimed in claim 9, wherein the first information processing apparatus transmits data P generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S2 and the received random number R2, to the second information processing apparatus, the second information processing apparatus transmits data Q generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the received random number S1 and the generated random number R1, to the second information processing apparatus, the first information processing apparatus generates the

encryption key K1 used for encrypting the data to be transmitted in the first transmission mode and the encryption key K2 used for encrypting the data to be transmitted in the second transmission mode in the case where data Q' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of the apparatus itself, the generated random number S1 and the received random number R1 is coincident with the received data Q, and the second information processing apparatus generates the encryption key K' used for decoding the data transmitted in the first transmission mode and the encryption key K'2 used for decoding the data transmitted in the second transmission mode in the case where data P' generated on the basis of the result of calculation of a unidirectional function using the information indicating the validity of
the apparatus itself, the received random number S2 and the generated random number R2 is coincident with the received data P (e.g. col. 6, lines 1-67, col. 7, lines 5-55).

In respect to claim 11, Traw and Nguyen disclose the information processing system as claimed in claim 9, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'I and the encryption key K'2, using a bit value of a part of the result of calculation of the unidirectional function (e.g. col. 6, lines 1-67, col. 7, lines 5-55).

In respect to claim 12, Traw and Nguyen disclose the information processing system as claimed in claim 11, wherein the first information processing apparatus and

the second information processing apparatus generate the data P, the data Q', the data Q and the data P', using a bit value of a part of the result of calculation of the unidirectional function (e.g., col. 6, lines 1-67, col. 7, lines 5-55).

In respect to claim 13, Traw and Nguyen disclose the information processing system as claimed in claim 11, wherein the first information processing apparatus and the second information processing apparatus generate the encryption key K1, the encryption key K2, the encryption key K'I and the encryption key K'2, using a feast significant n bits of the result of calculation of the unidirectional function (e.g. col. 6, lines 1-67 and col. 7, lines 5-55).

In respect to claim 14, Traw and Nguyen disclose the information processing system as claimed in claim 13, wherein the first information processing apparatus and the second information processing apparatus generate the data P, the data Q', the data Q' and the data P',

using a most significant m bits of the result of calculation of the unidirectional function (e.g. col. 7, lines 5-55).

In respect to claims 15-16, the claim limitations are similar to claims 9-11. Therefore claims 15-16 are rejected based on the similar rationale.

In respect to claim 17, Traw and Nguyen disclose the information processing system as claimed in claim 6, wherein the first information processing apparatus and the second information processing apparatus generate either one of the encryption key used for encrypting the data to be transmitted in the first transmission mode and the encryption key used for encrypting the data to be transmitted in the second transmission

mode, on the basis of the information indicating the validity of the apparatus itself, the generated random number and the received random number, and generate the encryption key of the other transmission mode on the basis of the generated encryption key; the generated random number and the received random number (e.g. col. 3, lines 10-30).

In respect to claims 18-27, the claim limitation is similar to claim 7-16. Therefore claim 18 is rejected based on the similar rationale.

In respect to claims 29-54 and 56-81, the claim limitations are similar to system claims 1-27. Therefore, claims 29-54 and 56-81 are rejected based on the similar rationale.

In respect to claims 28, 55 and 82, the claim limitations are similar to claim 1. Therefore, claims 28, 55 and 82 are rejected based on the similar rationale.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Examiner: Tongoc Tran
Art Unit: 2134

TT
July 11, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100